



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/847,813	05/01/2001	Curt Wohlgemuth	OMNI0008	6351

7590 12/07/2006

PERKINS COIE LLP
ATTN: Mr. Brian R. Coleman
101 Jefferson Drive
Menlo Park, CA 94025

EXAMINER

LANIER, BENJAMIN E

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 12/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/847,813	Applicant(s) WOHLGEMUTH ET AL.	
	Examiner Benjamin E Lanier	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 17 October 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3, 10-12, 19, 25 and 31-44 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3, 10-12, 19, 25 and 31-44 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.


Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.


KAMBIZ ZANDI
PRIMARY EXAMINER

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>5/15/06</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 13 October 2006 amends claims 1, 3, 10, 12, 19, 25, 31-33, 35, 36, 38-41, and 43. Applicant's amendments have been fully considered and are entered.

Response to Arguments

2. In response to Applicant Interview Summary, it was agreed that the Rothman reference did not include streaming software technology. No mention or discussion against Safadi was made. Therefore, Safadi still anticipates claims 31-42.
3. Applicant's argument that the amendments to claims 38 and 39 have overcome the 101 rejections is not persuasive because the claims are still claiming a propagated signal. Claims that recite nothing but the physical characteristics of a form of energy, such as a frequency, voltage, or the strength of a magnetic field, define energy or magnetism, per se, and as such are nonstatutory natural phenomena. O'Reilly, 56 U.S. (15 How.) at 112-14. Moreover, it does not appear that a claim reciting a signal encoded with functional descriptive material falls within any of the categories of patentable subject matter set forth in §101 (Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility Annex IV, Oct. 26, 2005, at http://www.uspto.gov/web/offices/pac/dapp/opla/preognotice/guidelines101_20051026.pdf, 1300 OG 142 (Nov. 22, 2005)).
4. Applicant's contention that "propagated data signals are physical (if ephemeral) structures that must be manufactured by a machine that is programmed to do so, either directly or indirectly, by a human," is not persuasive because The Supreme Court has read the term

Art Unit: 2132

“manufacture” in accordance with its dictionary definition to mean “the production of articles for use from raw or prepared materials by giving to these materials new forms, qualities, properties, or combinations, whether by hand-labor or by machinery.” Diamond v. Chakrabarty, 447 U.S. 303, 308, 206 USPQ 193, 196-97 (1980) (quoting American Fruit Growers, Inc. v Brogdex Co., 283 U.S. 1, 11, 8 USPQ 131, 133 (1931), which in turn, quotes the Century Dictionary). Other courts have applied similar definitions. See American Disappearing Bed Co. v. Arnaelsteen, 182 F.324, 325 (9th Cir. 1910), cert. denied, 220 U.S. 622 (1911). These definitions require physical substance, which a claimed signal does not have. Congress can be presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it reenacts a statute without change. Lorillard v. Pons, 434 U.S. 575, 580 (1978). Thus, Congress must be presumed to have been aware of the interpretation of manufacture in American Fruit Growers when it passed the 1952 Patent Act.

5. A manufacture is also defined as the residual class of product. 1 Chisum, §1.02[3] (citing W. Robinson, The Law of Patents for Useful Inventions 270 (1890)). A product is a tangible physical article or object, some form of matter, which a signal is not. That the other two products classes, machine and composition of matter, require physical matter. A signal, a form of energy, does not fall within either of the two definitions of manufacture. Thus, a signal does not fall within one of the four statutory classes of §101.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Art Unit: 2132

7. Claims 38, 39 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The added subject matter is: the computing system means for causing a functional change in the computing system. These means have not been identified in the claims or the specification.

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 38, 39 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. See MPEP § 2172.01. The omitted elements are: the computing system means for causing a functional change in the computing system.

Claim Rejections - 35 USC § 101

10. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

11. Claims 38 and 39 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed toward a propagated signal. Claims that recite nothing but the physical characteristics of a form of energy, such as a frequency, voltage, or the strength of a magnetic field, define energy or magnetism, per se, and as such are nonstatutory natural phenomena. O'Reilly, 56 U.S. (15 How.) at 112-14. Moreover, it

Art Unit: 2132

does not appear that a claim reciting a signal encoded with functional descriptive material falls within any of the categories of patentable subject matter set forth in §101 (Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility Annex IV, Oct. 26, 2005, at

http://www.uspto.gov/web/offices/pac/dapp/opla/preognotice/guidelines101_20051026.pdf,

1300 OG 142 (Nov. 22, 2005)).

12. The Supreme Court has read the term “manufacture” in accordance with its dictionary definition to mean “the production of articles for use from raw or prepared materials by giving to these materials new forms, qualities, properties, or combinations, whether by hand-labor or by machinery.” Diamond v. Chakrabarty, 447 U.S. 303, 308, 206 USPQ 193, 196-97 (1980) (quoting American Fruit Growers, Inc. v Brogdex Co., 283 U.S. 1, 11, 8 USPQ 131, 133 (1931), which in turn, quotes the Century Dictionary). Other courts have applied similar definitions. See American Disappearing Bed Co. v. Arnaelsteen, 182 F.324, 325 (9th Cir. 1910), cert. denied, 220 U.S. 622 (1911). These definitions require physical substance, which a claimed signal does not have. Congress can be presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change. Lorillard v. Pons, 434 U.S. 575, 580 (1978). Thus, Congress must be presumed to have been aware of the interpretation of manufacture in American Fruit Growers when it passed the 1952 Patent Act.

13. A manufacture is also defined as the residual class of product. 1 Chisum, §1.02[3] (citing W. Robinson, The Law of Patents for Useful Inventions 270 (1890)). A product is a tangible physical article or object, some form of matter, which a signal is not. That the other two products classes, machine and composition of matter, require physical matter. A signal, a form of energy,

Art Unit: 2132

does not fall within either of the two definitions of manufacture. Thus, a signal does not fall within one of the four statutory classes of §101.

Claim Rejections - 35 USC § 102

14. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

15. Claims 1-3, 10-12, 19, 25, 31-44 are rejected under 35 U.S.C. 102(e) as being anticipated by Vinson, U.S. Patent No. 6,453,334. Referring to claims 1, 10, Vinson discloses a method and apparatus to allow remotely located computer programs to be accessed on a local computer using a network file system that simulates a local drive on a client computer (Col. 1, lines 13-24 & Col. 2, lines 37-43), which meets the limitation of providing a network file system on a client. The user uses their web browser to navigate a web site, and clicks on link indicating a target program listed on a web page (Col. 5, lines 40-42). The link points to the index file for that target program. (Col. 5, lines 42-43). The web browser initiates retrieval of the index file, and based on the MIME type for the index file, knows that the index file should be downloaded to the client machine and the client agent started with the location of the index file given as an argument to the client agent (Col. 5, lines 43-52). When authenticated the FSD will add a newly created process to its list of processes that can access the files referenced by the index file (Col. 7, lines 28-37). All file operations are handled by the FSD, which downloads, caches, decompresses, and decrypts the pieces of the program as needed (Col. 7, lines 47-50), which meets the limitation of

Art Unit: 2132

wherein said network file system handles and forwards requests from streaming enabled local processes on said client that are directed at streaming software files located on said server. A deathwatch thread waits for a timeout when the time allowed for the process to access the program expires (Col. 8, lines 22-25), which meets the limitation of wherein said network file system examines said requests, and either grants or denies each of said requests depending on whether the request is justifiable from a security perspective by using information such as the history of previous access by the streaming enabled process. Furthermore, requests for access to the program are examined to see if the current process ID associated with the request is not in the process access list in the specified program descriptor block, and access is denied (Col. 14, lines 33-37), which meets the limitation of the nature of the originating streaming enabled process. For requests that contain a path, access will be granted to each top level directory in which the corresponding program descriptor block contains the current process ID in its process access list (Col. 14, lines 42-46), which meets the limitation of providing a network redirector component of said network file system. Requests that do not contain a path are handled on a case-by-case manner (Col. 14, lines 52-53), which meets the limitation of wherein said network redirector component makes visible to said network file system, a path that represents the server where said streaming software files are stored.

Referring to claims 2, 11, Vinson discloses that the FSD is called via a dispatch routine, which indicates that the newly created process is to be given access to the target program specified by the index file (Col. 7, lines 28-31), which meets the limitation of said network file system registers dispatch routines with the client operating system that handle zero or more common file operations selected from the group consisting of open, read, write, and close;

Art Unit: 2132

wherein a dispatch routine examines a file request and decides whether to grant or deny said file request. All operations are handled by the FSD, which downloads, caches, decompresses, and decrypts the pieces of the program as needed (Col. 7, lines 47-49 & Col. 13, lines 41-59), which meets the limitation of if said file request is granted then said dispatch routine forwards said file request to said server and sends back said server's response to said client operating system.

Referring to claims 3, 12, Vinson discloses that the user uses their web browser to navigate a web site, and clicks on link indicating a target program listed on a web page (Col. 5, lines 40-42). The link points to the index file for that target program. (Col. 5, lines 42-43). The web browser initiates retrieval of the index file, and based on the MIME type for the index file, knows that the index file should be downloaded to the client machine and the client agent started with the location of the index file given as an argument to the client agent (Col. 5, lines 43-52), which meets the limitation of when a local streaming enabled process on said client makes a file request for a streaming software file on said server. Dispatch routines are used by the FSD to receive information about the requested target file (Col. 6, lines 3-58), which meets the limitation of said client operating system calls a dispatch routine with said file request.

Referring to claims 19, 25, Vinson discloses a method and apparatus to allow remotely located computer programs to be accessed on a local computer using a network file system that simulates a local drive on a client computer (Col. 1, lines 13-24 & Col. 2, lines 37-43), which meets the limitation of providing a network file system on a client. The user uses their web browser to navigate a web site, and clicks on link indicating a target program listed on a web page (Col. 5, lines 40-42). The link points to the index file for that target program. (Col. 5, lines 42-43). The web browser initiates retrieval of the index file, and based on the MIME type for the

Art Unit: 2132

index file, knows that the index file should be downloaded to the client machine and the client agent started with the location of the index file given as an argument to the client agent (Col. 5, lines 43-52). When authenticated the FSD will add a newly created process to its list of processes that can access the files referenced by the index file (Col. 7, lines 28-37). All file operations are handled by the FSD, which downloads, caches, decompresses, and decrypts the pieces of the program as needed (Col. 7, lines 47-50), which meets the limitation of wherein said network file system handles and forwards requests from streaming enabled local processes on said client that are directed at streaming software files located on said server. A deathwatch thread waits for a timeout when the time allowed for the process to access the program expires (Col. 8, lines 22-25), which meets the limitation of wherein said network file system examines said requests, and either grants or denies each of said requests depending on whether the request is justifiable from a security perspective by using information such as the history of previous access by the streaming enabled process. Furthermore, requests for access to the program are examined to see if the current process ID associated with the request is not in the process access list in the specified program descriptor block, and access is denied (Col. 14, lines 33-37), which meets the limitation of the nature of the originating streaming enabled process. Vinson discloses that the FSD is called via a dispatch routine, which indicates that the newly created process is to be given access to the target program specified by the index file (Col. 7, lines 28-31), which meets the limitation of said network file system registers dispatch routines with the client operating system that handle zero or more common file operations selected from the group consisting of open, read, write, and close; wherein a dispatch routine examines a file request and decides whether to grant or deny said file request. All operations are handled by the FSD, which downloads, caches,

Art Unit: 2132

decompresses, and decrypts the pieces of the program as needed (Col. 7, lines 47-49 & Col. 13, lines 41-59), which meets the limitation of a dispatch routine examines a file request and decides whether to grant or deny said file request, and wherein if said file request is granted, then said dispatch routine allows the requested operation to proceed.

Referring to claim 31, Vinson discloses a method and apparatus to allow remotely located computer programs to be accessed on a local computer using a network file system that simulates a local drive on a client computer (Col. 1, lines 13-24 & Col. 2, lines 37-43), which meets the limitation of using a first computer to serve streaming software files to a second computer for streaming execution. The user uses their web browser to navigate a web site, and clicks on link indicating a target program listed on a web page (Col. 5, lines 40-42). The link points to the index file for that target program. (Col. 5, lines 42-43). The web browser initiates retrieval of the index file, and based on the MIME type for the index file, knows that the index file should be downloaded to the client machine and the client agent started with the location of the index file given as an argument to the client agent (Col. 5, lines 43-52). When authenticated the FSD will add a newly created process to its list of processes that can access the files referenced by the index file (Col. 7, lines 28-37). All file operations are handled by the FSD, which downloads, caches, decompresses, and decrypts the pieces of the program as needed (Col. 7, lines 47-50). A deathwatch thread waits for a timeout when the time allowed for the process to access the program expires (Col. 8, lines 22-25), which meets the limitation of using a filtering mechanism that is associated with said second computer for filtering requests for access to said streaming software files, wherein said filtering mechanism determines whether to grant requests for access to said streaming software files by determining one or more criteria from a set of criteria

Art Unit: 2132

comprising the history of previous access by the streaming enabled process. Furthermore, requests for access to the program are examined to see if the current process ID associated with the request is not in the process access list in the specified program descriptor block, and access is denied (Col. 14, lines 33-37), which meets the limitation of filtering access based on the nature of the originating streaming enabled process. For requests that contain a path, access will be granted to each top level directory in which the corresponding program descriptor block contains the current process ID in it's process access list (Col. 14, lines 42-46).

Referring to claims 32, 38, 40, Vinson discloses that all file operations are handled by the FSD, which downloads, caches, decompresses, and decrypts the pieces of the program as needed (Col. 7, lines 47-50), which meets the limitation of wherein said network file system handles and forwards requests from streaming enabled local processes on said client that are directed at streaming software files located on said server. A deathwatch thread waits for a timeout when the time allowed for the process to access the program expires (Col. 8, lines 22-25). Furthermore, requests for access to the program are examined to see if the current process ID associated with the request is not in the process access list in the specified program descriptor block, and access is denied (Col. 14, lines 33-37). For requests that contain a path, access will be granted to each top level directory in which the corresponding program descriptor block contains the current process ID in it's process access list (Col. 14, lines 42-46), which meets the limitation of providing information relating to one or more remote locations where streaming software files are stored, determining whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating

Art Unit: 2132

process exhibits a pre-determined pattern of piracy, and whether a section of said streaming software files that is being requested is a critical section that requires protection from piracy.

Referring to claim 33, 39, Vinson discloses that all file operations are handled by the FSD, which downloads, caches, decompresses, and decrypts the pieces of the program as needed (Col. 7, lines 47-50), which meets the limitation of wherein said network file system handles and forwards requests from streaming enabled local processes on said client that are directed at streaming software files located on said server. A deathwatch thread waits for a timeout when the time allowed for the process to access the program expires (Col. 8, lines 22-25). Furthermore, requests for access to the program are examined to see if the current process ID associated with the request is not in the process access list in the specified program descriptor block, and access is denied (Col. 14, lines 33-37). For requests that contain a path, access will be granted to each top level directory in which the corresponding program descriptor block contains the current process ID in it's process access list (Col. 14, lines 42-46). Vinson discloses that the FSD is called via a dispatch routine, which indicates that the newly created process is to be given access to the target program specified by the index file (Col. 7, lines 28-31), which meets the limitation of using dispatch routines for examining a request for access to said streaming software files, and after examining said request and if it is determined that a history of previous requests for access made by said originating process lacks a pre-determined pattern of piracy or that a section of said streaming software files that is being requested is a non-critical section, then forwarding said request to a corresponding remote server that is responsible for serving said streaming software files.

Referring to claim 34, Vinson discloses a method and apparatus to allow remotely located computer programs to be accessed on a local computer using a network file system that simulates a local drive on a client computer (Col. 1, lines 13-24 & Col. 2, lines 37-43), which meets the limitation of using a first computer to serve streaming software files to a second computer for streaming execution. The user uses their web browser to navigate a web site, and clicks on link indicating a target program listed on a web page (Col. 5, lines 40-42). The link points to the index file for that target program. (Col. 5, lines 42-43). The web browser initiates retrieval of the index file, and based on the MIME type for the index file, knows that the index file should be downloaded to the client machine and the client agent started with the location of the index file given as an argument to the client agent (Col. 5, lines 43-52). When authenticated the FSD will add a newly created process to its list of processes that can access the files referenced by the index file (Col. 7, lines 28-37). All file operations are handled by the FSD, which downloads, caches, decompresses, and decrypts the pieces of the program as needed (Col. 7, lines 47-50). A deathwatch thread waits for a timeout when the time allowed for the process to access the program expires (Col. 8, lines 22-25), which meets the limitation of using a filtering mechanism that is associated with said second computer for filtering requests for access to said streaming software files, wherein said filtering mechanism determines whether to grant requests for access to said streaming software files by determining one or more criteria from a set of criteria comprising the history of previous access by the streaming enabled process. Furthermore, requests for access to the program are examined to see if the current process ID associated with the request is not in the process access list in the specified program descriptor block, and access is denied (Col. 14, lines 33-37), which meets the limitation of filtering access based on the nature

Art Unit: 2132

of the originating streaming enabled process. For requests that contain a path, access will be granted to each top level directory in which the corresponding program descriptor block contains the current process ID in its process access list (Col. 14, lines 42-46). Requests that do not contain a path are handled on a case-by-case manner (Col. 14, lines 52-53), which meets the limitation of using a revealing mechanism to reveal to said client computer one or more remote locations on which said requested streaming software application program files are stored.

Referring to claims 35-37, Vinson discloses a method and apparatus to allow remotely located computer programs to be accessed on a local computer using a network file system that simulates a local drive on a client computer (Col. 1, lines 13-24 & Col. 2, lines 37-43). The user uses their web browser to navigate a web site, and clicks on link indicating a target program listed on a web page (Col. 5, lines 40-42). The link points to the index file for that target program. (Col. 5, lines 42-43). The web browser initiates retrieval of the index file, and based on the MIME type for the index file, knows that the index file should be downloaded to the client machine and the client agent started with the location of the index file given as an argument to the client agent (Col. 5, lines 43-52). When authenticated the FSD will add a newly created process to its list of processes that can access the files referenced by the index file (Col. 7, lines 28-37). All file operations are handled by the FSD, which downloads, caches, decompresses, and decrypts the pieces of the program as needed (Col. 7, lines 47-50), which meets the limitation of a processing device for processing a request for access to streaming software files stored on at least one server system that is remote from said processing device. A deathwatch thread waits for a timeout when the time allowed for the process to access the program expires (Col. 8, lines 22-25), which meets the limitation of wherein said processing device comprises a component that

Art Unit: 2132

determines whether to grant requests for access to said streaming software files based on whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said streaming software files that is being requested is a critical section that requires protection from piracy. Furthermore, requests for access to the program are examined to see if the current process ID associated with the request is not in the process access list in the specified program descriptor block, and access is denied (Col. 14, lines 33-37). For requests that contain a path, access will be granted to each top level directory in which the corresponding program descriptor block contains the current process ID in its process access list (Col. 14, lines 42-46). Requests that do not contain a path are handled on a case-by-case manner (Col. 14, lines 52-53), which meets the limitation of a redirector component that is associated with said processing device for informing said processing device of one or more locations in which said streaming software files are stored.

Referring to claim 41, Vinson discloses that all file operations are handled by the FSD, which downloads, caches, decompresses, and decrypts the pieces of the program as needed (Col. 7, lines 47-50), which meets the limitation of wherein said network file system handles and forwards requests from streaming enabled local processes on said client that are directed at streaming software files located on said server. A deathwatch thread waits for a timeout when the time allowed for the process to access the program expires (Col. 8, lines 22-25). Furthermore, requests for access to the program are examined to see if the current process ID associated with the request is not in the process access list in the specified program descriptor block, and access is denied (Col. 14, lines 33-37). For requests that contain a path, access will be granted to each

Art Unit: 2132

top level directory in which the corresponding program descriptor block contains the current process ID in it's process access list (Col. 14, lines 42-46). Vinson discloses that the FSD is called via a dispatch routine, which indicates that the newly created process is to be given access to the target program specified by the index file (Col. 7, lines 28-31), which meets the limitation of means for examining a request for access to said streaming software files, and means for determining whether said requests can be granted based on whether an originating process that is making said requests for access is a trusted process, that a history of previous requests for access made by said originating process lacks a pre-determined pattern of piracy or that a section of said streaming software files that is being requested is a non-critical section, a means for forwarding said request to a corresponding remote server that is responsible for serving said streaming software files.

Referring to claim 42-44, Vinson discloses that all file operations are handled by the FSD, which downloads, caches, decompresses, and decrypts the pieces of the program as needed (Col. 7, lines 47-50). A deathwatch thread waits for a timeout when the time allowed for the process to access the program expires (Col. 8, lines 22-25). Furthermore, requests for access to the program are examined to see if the current process ID associated with the request is not in the process access list in the specified program descriptor block, and access is denied (Col. 14, lines 33-37). For requests that contain a path, access will be granted to each top level directory in which the corresponding program descriptor block contains the current process ID in it's process access list (Col. 14, lines 42-46), which meets the limitation of providing information relating to one or more remote locations where streaming software files are stored, receiving a request from a computer process for access to said streaming software files, determining if a trusted

process/history of previous requests for access made by said computer process lacks a pre-determined pattern of piracy/critical section. All operations are handled by the FSD, which downloads, caches, decompresses, and decrypts the pieces of the program as needed (Col. 7, lines 47-49 & Col. 13, lines 41-59), which meets the limitation of if trusted process/history of previous requests of said computer process lacks a pre-determined pattern of piracy/critical section, then forwarding said request to a corresponding remote server that is responsible for serving said streaming software files.

16. Claims 31-44 are rejected under 35 U.S.C. 102(e) as being anticipated by Safadi, U.S. Patent No. 6,810,525. Referring to claim 31, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of using a first computer to serve said application program files to a second computer for execution, using a filtering mechanism that is associated with said second computer for filtering requests for access to said application program files, wherein said filtering mechanism determines whether to grant requests for access to said application program files by determining one or more criteria from a set of criteria comprising: a nature of an originating process that is making said requests for access, a history of previous requests for access made by said originating process, and a nature of a section of said application program files that is being requested. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 32, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be

Art Unit: 2132

authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored, determining whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claims 33, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17). The client application of Safadi would meet the limitation of the dispatch routine that examines the file requests and decides whether to grant or deny said file request (Col. 2, lines 1-10, Col. 3, lines 11-17). which meets the limitation of providing information relating to one or more remote locations where said application program files are stored, using dispatch routines for examining a request for access to said application program files, after examining said request and if it is determined that an originating process that is making said request for access is a trusted process, or that a history of previous requests for access made by said originating process lacks a pre-determined pattern of piracy, and that a section of said application program files that is being requested is a non-critical section, then forwarding said request to a corresponding remote server that is responsible for serving said

application program files. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 34, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of using a filtering mechanism on a client computer for filtering requests for access to said application program files, wherein said filtering mechanism determines whether to grant requests for access to said application program files by determining one or more criteria from a set of criteria comprising: a nature of an originating process that is making said requests for access, a history of previous requests for access made by said originating process, and a nature of a section of said application program files that is being requested. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of using a revealing mechanism to reveal to said client computer one or more remote locations on which said requested application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 35, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of a processing device

Art Unit: 2132

for processing a request for access to said application program files stored on at least one server system that is remote from said processing device, wherein said processing device comprises a component that determines whether to grant requests for access to said application program files based on: whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of a redirecting component that is associated with said processing device for informing said processing device of one or more locations in which said application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 36, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of processing means for processing a request for access to said application program files stored remotely from said processing means, wherein said processing means includes a determination whether to grant requests for access to said application program files based on: whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests

Art Unit: 2132

for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of a redirection means for revealing one or more locations in which said application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 37, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of a filtering means for filtering requests for access to said application program files stored remotely from said filtering means, wherein said filtering means includes an evaluation means for evaluating: an originating process that is making said requests for access, a history of previous requests for access made by said originating process, and a section of said application program files that is being requested. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of a redirection means for revealing one or more locations in which said requested application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 38, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of determining whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 39, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of using dispatch routines for examining a request for access to said application program files, after examining said request and if it is determined that an originating process that is making said request for access is a trusted process, and that a history of previous requests for access made by said originating process lacks a pre-determined pattern of piracy, and that a section of said application

Art Unit: 2132

program files that is being requested is a non-critical section, then forwarding said request to a corresponding remote server that is responsible for serving said application program files. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 40, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of determining whether an originating process that is making said request for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 41, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of a means for examining requests for access to said application program files, a means for determining whether said requests can be granted based on whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a predetermined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy, if said requests are granted then forwarding said requests to a corresponding server that is responsible for serving said application program files. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of a means for providing location information to a local computing system of said application program files that are stored on one or more remote locations. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 42-44, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of receiving a request from a computer process for access to said application program files, determining if said

Art Unit: 2132

computer process that is making said request for access is a trusted process, if said computer process is a trusted process, then forwarding said request to a corresponding remote server that is responsible for serving said application program files. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Raz, U.S. Patent No. 6,311,221

Eylon, U.S. Patent No. 6,574,618

Eylon, U.S. Patent No. 6,757,894

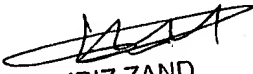
18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


Benjamin E. Lanier


KAMBIZ ZAND
PRIMARY EXAMINER